DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
2300 E STREET NW
WASHINGTON DC 20372-5300

IN REPLY REFER TO
BUMEDINST 5236.2
BUMED-M09B6
1 Oct 2008

BUMED INSTRUCTION 5236.2

From: Chief, Bureau of Medicine and Surgery

Subj: ARMED FORCES HEALTH LONGITUDINAL TECHNOLOGY APPLICATION (AHLTA) END USER DEVICE STANDARD CONFIGURATION POLICY

Ref: (a) OMB memo M-07-11 of 22 Mar 07 (NOTAL)
(b) OMB memo M-07-18 of 1 Jun 07 (NOTAL)
(c) OASD(HA) memo of 3 Aug 07 (NOTAL)
(d) OASD(HA) memo 3 Aug 07 (NOTAL)
(e) OASD(HA) memo 3 Aug 07 (NOTAL)
(f) OASD(HA) memo 3 Aug 07 (NOTAL)
(g) ASD(HA) memo 1 Oct 07 (NOTAL)
(h) Navy Medicine Information Management/Information Technology Integrated Process Team Concept of Operations, 2 Jun 2006 (NOTAL)

Encl: (1) Glossary of Terms

1. Purpose

a. To establish policy and guidance for Navy Medicine (NAVMED) governing the use of a standard hardware and software baseline core configuration for AHLTA desktop, notebook, and tablet end user devices (EUD) consistent with the adoption of TRICARE Management Activity (TMA) guidance, Department of Defense (DoD) standards of operation, and Federal Desktop Core Configuration guidelines.

b. To assign responsibilities within NAVMED for the evaluation, registration, and implementation of AHLTA EUDs baseline core configurations.

c. To implement policy and guidance across the NAVMED enterprise consistent with references (a) through (f), intended to simplify procurement activities and promote seamless interoperability both within the Military Health System (MHS) and between MHS and other DoD components.

2. Background

a. In accordance with reference (g), the Assistant Secretary of Defense for Health Affairs directed each Service to provide a written policy detailing single standard hardware and software configuration for AHLTA EUDs to improve application management and troubleshooting, facilitate ordering processing, minimize hardware and software conflicts, and optimize performance.

b. For centrally-managed programs, TMA requires all desktops to be in compliance with the security configuration requirements of references (a) and (b) to improve information security, acquisition, deployment, and configuration management of EUD hardware and software.

c. NAVMED's environment is driven by business and operational requirements and faces additional challenges due to integration with other DoD, Federal, and commercial agencies. These challenges demand a comprehensive approach to standardization and configuration management.

3. Applicability and Scope

a. Applies to all NAVMED healthcare providers, support and administrative staff that access AHLTA.

b. Applies to all AHLTA specific EUD hardware and software configurations across the NAVMED enterprise. This includes, but is not limited to, desktop workstations, portable devices (notebooks and tablet personal computers (PCs)), and other wireless devices capable of storing, processing, or transmitting AHLTA data.

4. Glossary of Terms. Terms used in this instruction are defined in enclosure (1).

5. Policy

a. Precedence. This instruction is consistent with TMA and DoD policies related to AHLTA hardware and software application standard minimum guidance and operating system security configuration.

b. Secure Deployment

(1) AHLTA EUD core configurations will be deployed securely using a controlled, standardized, and approved enterprise infrastructure approach. Reference (h) established the NAVMED Information Management/Information Technology (IM/IT) Integrated Product Team concept of operations to address specific governance, organizational alignment, and portfolio management processes.

(2) As part of the IM/IT governance framework, the NAVMED IT Configuration Control Board (ITCCB), will provide a forum for evaluation and approval of technical configurations for management standards across the enterprise. The AHLTA EUD baseline hardware and software core configurations to include at a minimum: desktop, tablet, notebook, and software, will be evaluated and approved by the NAVMED ITCCB prior to deployment. Software applications that have been registered and approved by the NAVMED ITCCB may be added to this baseline configuration to meet mission requirements.

c. Frequency Management. This instruction will be updated annually or more frequently as required to reflect advances in technology, product availability, and market support.

6. Responsibilities. All addressees shall implement the guidance set forth in this instruction within their organizations and shall ensure sufficient allocation of resources for implementing all requirements contained in this instruction, and contact the BUMED CIO Officer for further guidance, as needed.

a. The Bureau of Medicine and Surgery Command Information Officer (BUMED CIO) shall provide strategic oversight and instruction for a standard and controlled EUD baseline core configuration solution across the enterprise.

b. The NAVMED ITCCB shall:

(1) Develop guidance and procedures to implement and enforce this instruction.

(2) Issue a standard AHLTA hardware desktop configuration.

(3) Issue a standard AHLTA notebook and tablet configuration.

(4) Issue a standard AHLTA software configuration.

(5) Approve or disapprove hardware and software applications that will change the baseline standard configuration.

c. All NAVMED purchasing authorities shall be consistent with this instruction, integrating guidance as defined by NAVMED ITCCB into all new acquisitions of AHLTA EUDs to include reference (b) which states DoD agencies shall adopt the standard security configurations for Windows XP and VISTA operating systems.

d. NAVMED Information System Support Activity shall monitor all new AHLTA EUD procurements for compliance with this instruction and related policies, procedures, standards, and guidelines to include:

(1) Ensuring compliance with guidance concerning the monitoring of AHLTA EUD hardware and software baseline core configurations.

(2) Compliance with this instruction and the evaluation and validation requirements that will be forthcoming from NAVMED ITCCB and this instruction.

e. Each Region and NAVMED subordinate command Information Systems Officer (ISO) shall:

(1) Ensure that software and hardware baseline core configurations as defined by NAVMED ITCCB are integrated as part of all new and legacy NAVMED AHLTA EUDs.

(2) Upon request, provide to the BUMED CIO via the Regional ISO, specific implementation timelines for legacy system compliance with this instruction.

7. Point of contact. BUMED CIO at (202) 762-3180/DSN 762-3180.

A. M. ROBINSON, JR.

Distribution:
SNDL, FH (NAVMED)
C52 (NAVMEDCLINIC)

Distribution is electronic only via the Navy Medicine Web site at:
http://navymedicine.med.navy.mil/default.cfm?selTab=Directives

GLOSSARY OF TERMS

Configuration Control Board (CCB). The CCB is a cross-functional group set up to evaluate change requests for business need, priority, cost/benefit, and potential impacts to existing systems and/or processes. Additionally, the CCB is responsible for approving or rejecting proposed changes in an effort to maintain a stable, available, and reliable IT infrastructure capable of meeting NAVMED functional requirements and performance expectations.

End User Device (EUD). An end user device is, but not limited to, PCs, workstations, and other desktop machines dedicated to a single user's activity, as well as mobile devices such as PEDs, laptops, and tablets.

Federal Desktop Core Configuration (FDCC). Designed to provide a single standard enterprise-wide managed environment for desktops, notebooks, and tablet PCs running Microsoft Windows operating system.

Table Personal Computer (PC). Allows the user to take notes using natural handwriting on a touch screen that is stylus or digital pen-sensitive. It functions both as the user's primary personal computer and as a note-taking device.

Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to Personal Data Assistants (PDA), cellular, PCS telephones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

Information Systems Officer (ISO). Coordinate and collaborate on IM/IT issues, information assurance, computing and communication infrastructure, implementation and operations.